Polynomials over {0,1}

Emanuele Viola

Northeastern University
work done at Columbia, IAS, and Harvard

October 2008

Polynomials

- Polynomials:

  degree d, n variables over $F_2 = \{0,1\}$

  E.g., $p = x_1 + x_5 + x_7$ degree $d = 1$

  $p = x_1 \cdot x_2 + x_3$ degree $d = 2$

- Computational model: $p : \{0,1\}^n \to \{0,1\}$

  Sum (+) = XOR, Product ($\cdot$) = AND

  $x^2 = x$ over $F_2 \Rightarrow$ Multilinear

- Complexity = degree

Motivation

- Coding theory

  Hadamard, Reed-Muller codes based on polynomials

- Circuit lower bounds [Razborov '87; Smolensky '87]

  Lower bound on polynomials $\Rightarrow$ circuit lower bound

- Pseudorandomness [Naor & Naor '90]

  Useful for algorithms, PCP, expanders, learning…

Outline

- Overview
- Correlation bounds
- Pseudorandom generators

Lower bound

- Question: Which functions cannot be computed by low-degree polynomials?

- Answer:

  $x_1 \cdot x_2 \cdots x_d$ requires degree d

  Majority$(x_1,\ldots,x_n) := 1 \Leftrightarrow \Sigma\, x_i > n/2$
  requires degree n/2

Correlation bound

- Question: Which functions do not correlate with low-degree polynomials?

- $\mathrm{Cor}(f,\text{degree } d) := \max_{\text{degree-}d\ p} \mathrm{Bias}(f+p) \in [0,1]$

  $\mathrm{Bias}(f+p) := |\ \Pr_{U \in \{0,1\}^n}[f(U)=p(U)] - \Pr_U[f(U) \neq p(U)]\ |$

  E.g. $\mathrm{Cor}(\text{deg. } d, \text{deg. } d) = 1$; $\mathrm{Cor}(\text{random } f, \text{deg. } d) \approx 0$

- Want: correlation small, degree large.

- Barrier: $\exists$ explicit n-bit f : $\mathrm{Cor}(f, \text{degree } \log_2 n) \leq 1/n$?

A sample of correlation bounds

- [Babai, Nisan and Szegedy '92, Bourgain '05, Green Roy Straubing '05]:
  Explicit f: Cor(f,degree $0.1\log n$) $\leq \exp(-n)$

- [Razborov '87]: Explicit f : Cor(f, degree $n^{1/3}$) $\leq 1/\sqrt{n}$

- Hardness amplification question:
  Can amplify Razborov's bound to break the "Cor(f, degree $\log n$) $\leq 1/n$" barrier?

Yao's XOR lemma

- Generic way to boost correlation bound

  M = computational model (e.g. M = degree log n)

- $f^{\oplus k}(x_1,\ldots, x_k) := f(x_1) \oplus \cdots \oplus f(x_k)$

  Hope: $\mathrm{Cor}(f^{\oplus k}, M) \leq \mathrm{Cor}(f,M)^{\Omega(k)}$

- Theorem [Yao, Levin, Goldreich Nisan Wigderson, Impagliazzo,…]

  XOR lemma for M = circuits

- Question: [Razborov] bound for f + XOR lemma $\Rightarrow$

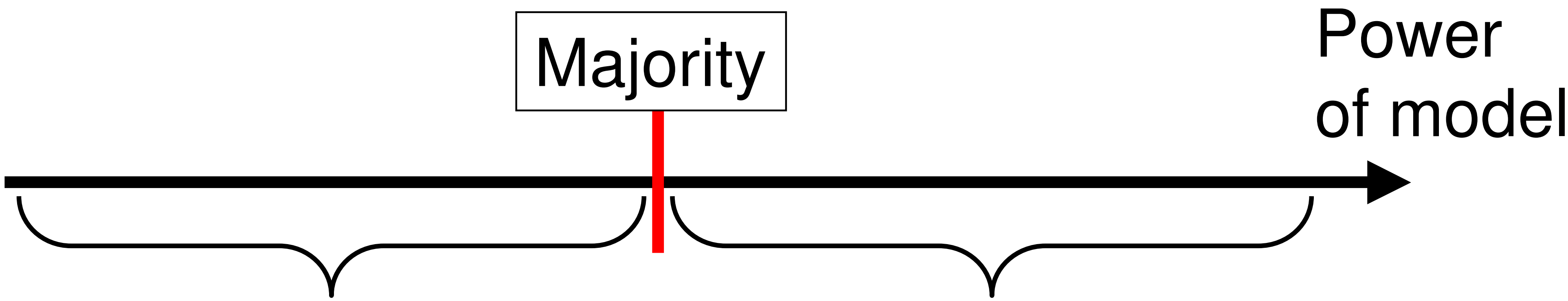
  $\mathrm{Cor}(\, f(x_1) \oplus \cdots \oplus f(x_k)$, degree log n $) << 1/n$?

XOR lemma proofs require majority

- XOR lemma proofs [L,GNW,I,…] are code-theoretic
- Theorem [Shaltiel V. ’07]: Code-theoretic proofs of XOR lemma require model to compute majority
- Since polynomials cannot compute majority, no code-theoretic proof of XOR lemma for polynomials

[Shaltiel V. '07] + [Razborov Rudich] + [Naor Reingold]

"Lose-lose" reach of standard techniques:



Cannot prove
XOR lemma
[Shaltiel V.]

Cannot prove
Correlation bounds
[RR] + [NR]
``natural proofs barrier''

"You can only amplify the hardness you don't know"

Where we are

- Theorem[Shaltiel V. '07]: Code-theoretic proofs of XOR lemma do not work for polynomials

- Open: XOR lemma for degree log n

- Note: XOR lemma trivially true for degree 0, 1

- Next[V. Wigderson]: XOR lemma for any constant degree
  Proof not code-theoretic

XOR lemma for constant degree

- Theorem[V. Wigderson]: XOR lemma for degree O(1)

- Technique: Use norm $N(f) \approx [0,1]$:

  (I) $\mathrm{Cor}(f,\text{degree } d) \approx N(f)$

  (II) $N(f^{\oplus k}) = N(f)^k$

- Proof of the XOR lemma:

$$\mathrm{Cor}(f^{\oplus k},\text{degree } d) \approx N(f^{\oplus k}) = N(f)^k \approx \mathrm{Cor}(f,\text{degree } d)^k$$

Q.e.d.

Gowers norm

[Gowers '98; Alon Kaufman Krivelevich Litsyn Ron '03]

- Measure correlation with degree-d polynomials: check if random d-th derivative is biased

- Derivative in direction $y \in \{0,1\}^n$: $D_y\, p(x) := p(x+y) - p(x)$
  - E.g. $D_{y_1\, y_2\, y_3}(x_1\, x_2 + x_3) = y_1 x_2 + x_1 y_2 + y_1 y_2 + y_3$

- Norm $N_d(p) := E_{Y^1 \ldots Y^d \in \{0,1\}^n} \mathrm{Bias}_U[D_{Y^1 \ldots Y^d}\, p(U)] \in [0,1]$

(Bias [Z] := | Pr[Z = 0] - Pr[Z = 1] |)

$N_d(p) = 1 \Leftrightarrow$ p has degree d

- From combinatorics [Gowers; Green Tao], to PCP [Samorodnitsky Trevisan], to correlation bounds [**V.** Wigderson]

Properties of norm

- $N_d(p) := E_{Y^1 \ldots Y^d \in \{0,1\}^n} \text{Bias}_U[D_{Y^1 \ldots Y^d}\, p(U)]$

(I) $N_d(f) \approx$ Cor(f,degree d) :

Lemma[Gowers, Green Tao]:

Cor(f,degree d) $\leq N_d(f)^{1/2^d}$

Lemma[Alon Kaufman Krivelevich Litsyn Ron]:

(Gowers inverse conjecture, $N \approx 1$ case)

Cor(f,degree d) $\leq 1/2 \Rightarrow N_d(f) \leq 1-2^{-d}$

(II) $N(f^{\oplus k}) = N(f)^k$

Follows from definition

Proof of XOR lemma

(I) $N_{d+1}(f) \approx$ Cor(f,degree d) :

Lemma[G, GT]: Cor(f,degree d) $\leq N_d(f)^{1/2^d}$

Lemma[AKKLR]: Cor(f,degree d) $\leq 1/2 \Rightarrow N_d(f) \leq 1-2^{-d}$

(II) $N(f^{\oplus k}) = N(f)^k$

- Theorem[V. Wigderson]:

  Cor(f,deg. d) $\leq 1/2 \Rightarrow$ Cor($f^{\oplus k}$,deg. d) $\leq \exp(-k/4^d)$

- Proof:

  Cor($f^{\oplus k}$,deg. d) $\leq N_d(f^{\oplus k})^{1/2^d} = N_d(f)^{k/2^d} \leq (1-2^{-d})^{k/2^d}$

  Q.e.d.

- More[VW]: Best known bound for degree 0.5 log n, …

Outline

- Overview

- Correlation bounds

- Pseudorandom generators

Pseudorandom generator

[Blum Micali; Yao; Nisan Wigderson]

$$\overbrace{010110}^{s(n)} \longrightarrow \boxed{\textbf{Gen}} \longrightarrow \overbrace{100110\cdots01100}^{n}$$

- Efficient

- Short seed s(n) << n

- Output "fools" degree-d polynomial p

$$| \text{Bias}_{X\in\{0,1\}^s}[p(\text{Gen}(X))] - \text{Bias}_{U\in\{0,1\}^n}[p(U)] | \leq \varepsilon$$

Previous results

- Th.[Naor Naor '90]: Fools linear, seed = $O(\log n/\varepsilon)$
  - Applications: derandomization, PCP, expanders, learning…
- Th.[Luby Velickovic Wigderson '93]:
  Fools constant degree, seed = $\exp(\sqrt{\log n/\varepsilon})$
  - [V. '05] gives modular proof of more general result
- Th.[Bogdanov '05]: Any degree, but over large fields
- Over small fields such as {0,1}:

  no progress since 1993, even for degree d=2

Our results

- To fool degree d:
  Let $L \in \{0,1\}^n$ fool linear polynomials [NN]
  bit-wise XOR d independent copies of L:

$$\boxed{\text{Generator} := L^1 + \ldots + L^d}$$

- Theorem[Bogdanov V.]:
  (I) Unconditionally: Fool degree d = 2, 3
  (II) Under "d vs. d-1 inverse conjecture": Any degree

- Optimal seed $s = O(\log n)$ for fixed degree and error

Recent developments after [BV]

- Th.[Lovett]: The sum of 2^d generators for degree 1 fools degree d, unconditionally.
  - Recall [BV] sums d copies

- Progress on "d vs. d-1 inverse conjecture":

- Th.[Green Tao]: True when $|F| > d$
  Proof uses techniques from [BV]
  [BV] works when $|F| > d$ or $d = 2,3$

- Th. [Green Tao], [Lovett Meshulam Samorodnitsky]:
  False when $F = \{0,1\}$, $d = 4$

Our latest result

- Theorem[V.]:
  The sum of d generators for degree 1
  fools polynomials of degree d.
  For every d and over any field.

  (Despite the inverse conjecture being false)

- Improves on both [Bogdanov V.] and [Lovett]

- Also simpler proof

Proof idea

- Recall: want to show the sum of d generators for degree 1 fools degree-d polynomial p

- Induction: Fool degree d $\Rightarrow$ fool degree-(d+1) p

  Inductive step: Case-analysis based on
  Bias(p) := $| \Pr_{U \in \{0,1\}^n} [p(U)=1] - \Pr_U [p(U)=0] |$

  Cases:
- Bias(p) negligible $\Rightarrow$ Fool p using extra copy of generator for degree 1

- Bias(p) noticeable $\Rightarrow$ p close to degree-d polynomial $\Rightarrow$ fool p by induction

Case Bias(p) negligible

- Hypothesis: $L^1, \ldots, L^d$, L over $\{0,1\}^n$ fool degree 1

  $W := L^1 + \cdots + L^d$ fools degree d

- Goal: For degree-(d+1) p: Bias (p(W+L)) ≈ Bias (p(U))

- Lemma[V]: Bias (p(W + L)) ≤ Bias (p(U)) ≈ 0

- Proof: $\mathrm{Bias}_{W,L}\, [p(W + L)]^2 = E_W [\, \mathrm{Bias}_L\, (p(W{+}L))\,]^2$

$$\leq E_W [\, \mathrm{Bias}_{L,L'}\, \underbrace{(p(W{+}L) + p(W{+}L'))}_{\text{degree d in W}}\,]$$

$$\approx E_U [\, \mathrm{Bias}_{L,L'}\, (p(U{+}L) + p(U{+}L'))\,] \approx \mathrm{Bias}_U(p)^2$$

Q.e.d.

Case Bias(p) noticeable

- Bias(p) noticeable; p has degree d+1

- p noticeably correlates with constant (51 %)

Self-correction [Bogdanov V.]
This result used in [Green Tao]

- p highly correlates with (function of) degree-d polynomials (99 %)

- Apply induction

Recent applications

- Fool width-2 read-d branching programs
  [Bogdanov Dvir Verbin Yehudayoff]

- Polynomial reconstruction problem
  [Gopalan Khot Saket]

- Degree bounds for annihilating polynomials
  Given $p_1,\ldots,p_t$, what is min. deg. of $q : q(p_1,\ldots,p_t) = 0$?

  formal [Dvir Gabizon Wigderson, Kayal]
  informal [Mossel Shpilka Trevisan, Shpilka] + [BV, L, V]

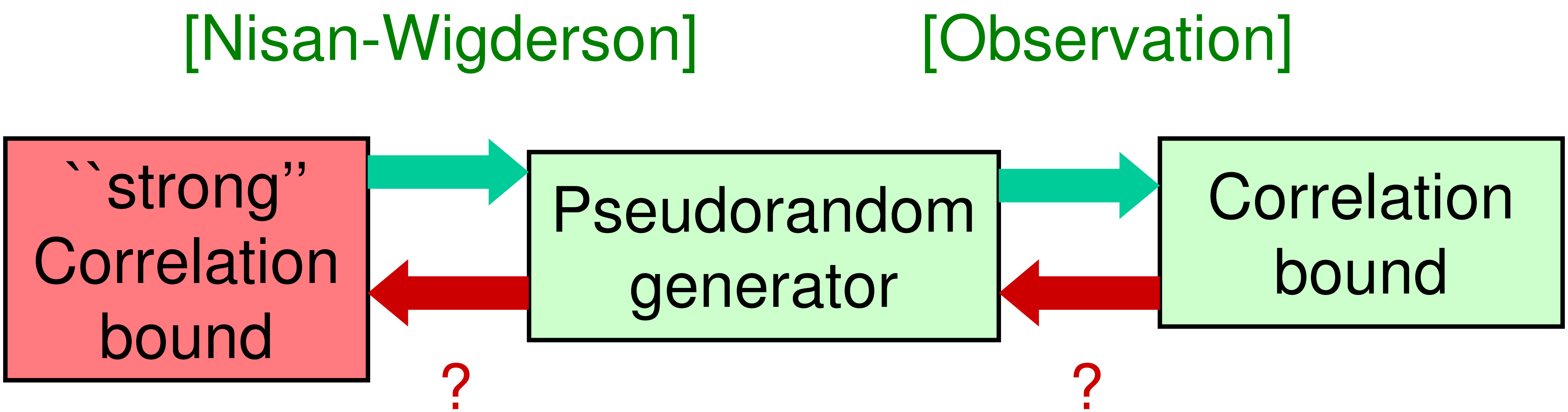
What we have seen

- Computational model: degree-d polynomials over F_2
  Arises in codes, lower bounds, pseudorandomness

- Correlation bounds
  Standard XOR lemma does not work [Shaltiel V.]
  XOR lemma for constant degree [V. Wigderson]

- Pseudorandom generators
  Recent developments [BV,L,GT,LMS]
  Sum of d generators for degree 1 fools degree d [V.]

Open problems



- Still open: Understand these connections